

Daniel E. Geer Jr. In-Q-Tel

Less Is More:

Saving the Internet from Itself

he more numerous the targets, the more certain that attackers will appear. Accelerating the interconnection of indefensible targets shortens the interval over which attackers appear, while increasing the variety of pathways they might use to attack. Neither of these observations is new, nor specific to cybersecurity and computer systems. They are natural processes.

There have now been a number of "natural experiments" on how increasing populations of insecure yet interconnected systems draw attackers. Changing this dynamic will require changing how we operate; bearing down harder on what we do now won't produce a change. Trite as it sounds, we can't keep doing the same thing in hopes of a better result. The cyber arena is offense dominant and always will be.

"Saving the Internet" in the present context requires value judgments about what is worth saving. Do you leave the burning house with your mother's silver or with your tax records, with your dog or with your keychains? We can't save everything, so what's worth saving and what can we tolerably spend (or lose) in pursuit of that goal?

Empires have fallen when they were overextended, when they captured territory they couldn't retain. Businesses likewise. The Internet is overextending as we speak. The process of extension is everywhere, and we have to modify the critical aspects of that extension before we cross various points of irreversibility.

We have to do this while there is still any choice to be made. The central dynamic of extension is competition. Competition in the physical world can certainly be vicious, but it also has physical limits. This is less true for Internet competition, as inherent limitations of time, place, speed, and reach don't apply.

What does apply with the Internet is the creation of targets of opportunity. Studies of attacker economics have shown that market size is the core driver of attacks—the more targets of like exploitability, the more

an investment in attack tooling is profitable and thus inevitable. This is natural. As ecologist Thomas Ray noted, every successful system accumulates parasites. At the same time, nature's response is neither predictable nor centrally governed, but rather unpredictable and locally governed—that is to say, mutation-fueled natural selection.

There's no doubt that increasingly powerful, location-independent technology in the hands of the many changes the distribution of power. But the power that is growing on the Internet will soon surpass the ability of our existing institutions to modify it in any meaningful way. The Internet must be broken up into governable chunks, or it becomes government.

This is the choice: Do we want to make protection of individual Internet elements the owners' problem for all values of "owner," subject to unpredictable differentiation and a picking of winners and losers by emergent processes that we can perhaps still influence but never again control? Or do we want near monocultures of a few winning platforms whose vastness represents empire and thus requires a level of defense that only a nation-state can provide, if at all?

n the former lies the path of so much science fiction, especially if the Singularity is imminent. On the latter lies the path to a state-level control far more invasive than fiat currency and secret standing armies. If neither of these options appeals, now is the time to apply the brakes. Now is the time, individually and collectively, to tamp down risk by tamping down dependence on the Internet. Now is the time to say that target richness is a disease for which the cure is intolerable.

Daniel E. Geer Jr. is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at dan@geer.org.